CLAIMS

What is claimed is:

1. In a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for a source computing system constructing an electronic message, the method comprising the following:

an act of designating at least one destination address in the electronic message, the destination address corresponding to one or more recipient computing devices;

an act of including a first security token in a header portion of the electronic message, the first security token being at least derived from a first credential of a first credential type; and

an act of including a second security token in the header portion of the electronic message, the second security token being at least derived from a second credential of a second credential type.

2. The method in accordance with Claim 1, wherein the first security token is biometric data.

3. The method in accordance with Claim 1, further comprising the following:

an act of including an encryption manifest in the header portion to thereby designate portions of a body portion of the electronic message that are encrypted.

4. The method in accordance with Claim 1, further comprising the following:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

an act of transmitting the electronic message with the first security token and the second security token in the header portion to the one or more recipient computing devices.

5. The method in accordance with Claim 1, wherein the first security token is the first credential.

6. The method in accordance with Claim 1, wherein the first security token is a first signature that was generated using the first credential.

7 The method in accordance with Claim 6, further comprising the following:

an act of including the first credential in the electronic message.

8. The method in accordance with Claim 1, wherein the second security token is the second credential.

9. The method in accordance with Claim 1, wherein the second security token is a second signature that was generated using the second credential.

10. The method in accordance with Claim 9, further comprising the following:

an act of including the second credential in the electronic message.

11. The method in accordance with Claim 1, wherein the at least one destination address corresponds to at least a first and a second recipient computing system, the first

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

computing system using the first credential to identify the source computing system, and the second computing system using the second credential to identify the source computing system.

12. The method in accordance with Claim 11, further comprising the following:

an act of determining that the first recipient computing system uses the first credential to identify the source computing system; and

an act of determining that the second recipient computing system uses the second credential to identify the source computing system.

13. The method in accordance with Claim 1, wherein the at least one destination address corresponds to at least a first recipient computing system that uses both of the first credential and the second credential to identify the source computing system.

14. The method in accordance with Claim 13, further comprising the following:

an act of determining that the first recipient computing system uses both of the first credential and the second credential to identify the source computing system.

15. The method in accordance with Claim 1, wherein the at least one destination address corresponds to at least a first recipient computing system that uses the first credential and the second credential to identify the source computing system, the electronic message also traversing through an intermediary computing system that uses the second credential to identify the source computing system.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

16. The method in accordance with Claim 15, further comprising the following:

an act of determining that the first recipient computing system uses the first credential to identify the source computing system; and

an act of determining that the intermediary computing system uses the second credential to identify the source computing system.

17. The method in accordance with Claim 15, further comprising:

an act of designating an intermediary address that corresponds to the intermediary computing device.

18. The method in accordance with Claim 1, further comprising

an act of encoding the first security token;

an act of including, in the header portion, an identification of an encoding format of the first security token; and

an act of including, in the header portion, an identification of a type of the security token.

19. The method in accordance with Claim 18, wherein the security token comprises a credential.

20. The method in accordance with Claim 1, wherein the first security token is a signature generated by a user, the method further comprising:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

an act of generating a reference indicating where a credential associated with the user may be found;

an act of including the reference in the header portion of the electronic message.

21. The method in accordance with Claim 1, wherein the electronic message is a Simple Object Access Protocol (SOAP) envelope in which the header portion is the header portion of the SOAP envelope.

22. The method in accordance with Claim 1, wherein the electronic message is a HyperText Transport Protocol (HTTP) message, and wherein the header portion is a header portion of the HTTP message.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

23. A computer program product for use in a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, the computer program product for implementing a method for a source computing system constructing an electronic message, the computer program product comprising one or more computer-readable media have thereon the following:

computer-executable instructions for designating at least one destination address in the electronic message, the destination address corresponding to one or more recipient computing devices;

computer-executable instructions for including a first security token in a header portion of the electronic message, the first security token being at least derived from a first credential of a first credential type; and

computer-executable instructions for including a second security token in the header portion of the electronic message, the second security token being at least derived from a second credential of a second credential type.

24. The computer program product in accordance with Claim 23, wherein the one or more computer-readable media are physical storage media.

25. The computer program product in accordance with Claim 23, wherein the one or more computer-readable media further have thereon the following:

computer-executable instructions for determining that a first recipient computing system uses the first credential to identify the source computing system; and

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

computer-executable instructions for determining that a second recipient computing system uses the second credential to identify the source computing system.

26. The computer program product in accordance with Claim 23, wherein the one or more computer-readable media further have thereon the following:

computer-executable instructions for determining that a first recipient computing system uses both of the first credential and the second credential to identify the source computing system.

27. The computer program product in accordance with Claim 23, wherein the one or more computer-readable media further have thereon the following:

computer-executable instructions for determining that a first recipient computing system uses the first credential to identify the source computing system; and

computer-executable instructions for determining that an intermediary computing system uses the second credential to identify the source computing system.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

28. One or more computer-readable media having stored thereon a data structure that represents an electronic message, the electronic message including a header field and a body field, the header field including the following:

a first data field that represents at least one destination address in the electronic message, the destination address corresponding to one or more recipient computing devices;

a second data field that represents a first security token in a header field, the first security token being at least derived from a first credential of a first credential type; and

a third data field that represents a second security token in the header field, the second security token being at least derived from a second credential of a second credential type.

29. The one or more computer-readable media of Claim 28, wherein the second data field represents the first credential.

30. The one or more computer-readable media of Claim 28, wherein the second data field represents a signature that was generated using the first credential.

31. The one or more computer-readable media of Claim 30, wherein the header field further comprises the following:

a fourth data field that represents the first credential.

32. The one or more computer-readable media of Claim 30, wherein the third data field represents a signature that was generated using the second credential.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

33. The one or more computer-readable media of Claim 32, wherein the header field further comprises the following:

a fourth data field that represents the second credential.

34. The one or more computer-readable media of Claim 30, further comprising a body field, wherein the header field further comprises the following:

a fourth data field that represents an encryption manifest identifying portions of the body field that are encrypted.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

35. A computer program product for use in a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for identifying a source computing system of an electronic message, the computer program product comprising one or more computer-readable media having stored thereon the following:

computer-executable instructions for detecting the receipt of an electronic message;

computer-executable instructions for selecting one of a plurality of credentials included in a header portion of the electronic message; and

computer-executable instructions for identifying the source computer system using the selected credential.

36. A computer program product in accordance with Claim 35, wherein the one or more computer-readable media are physical storage media.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

37. A computer program product for use in a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for identifying a source computing system of an electronic message, the computer program product comprising one or more computer-readable media having stored thereon the following:

computer-executable instructions for detecting the receipt of an electronic message;

computer-executable instructions for reading a credential from the electronic message;

computer-executable instructions for determining how to handle the credential and the electronic message based on a position of the credential within a logical hierarchical tree of credentials.

computer-executable instructions for handling the credential and the electronic message as determined.

38. A computer program product in accordance with Claim 37, wherein the one or more computer-readable media are physical storage media.

39. A computer program product in accordance with Claim 37, wherein the computer-executable instructions for determining how to handle the credential and the electronic message comprise the following:

computer-executable instructions for consulting handling rules of at least one ancestral credential in the logical hierarchical tree;

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

computer-executable instructions for consulting extended handling rules specific to the credential included in the electronic message; and

computer-executable instruction for determining handling rules for the credential included in the electronic message by using the handling rules for the at least one ancestral credential as well as the extended handling rules specific to the credential included in the electronic message.

40. The computer program product in accordance with Claim 37, wherein the credential includes biometric data.

41. The computer program product in accordance with Claim 37, wherein the electronic message is a Simple Object Access Protocol (SOAP) envelope, and wherein the credential is included in a header portion of the SOAP envelope.

42. The computer program product in accordance with Claim 37, wherein the electronic message is a HyperText Transport Protocol (HTTP) message, and wherein the credential is included in a header portion of the HTTP message.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

43. One or more computer-readable media having stored thereon a data structure, the data structure comprising the following:

a first data field that represents a first credential;

a second data field that represents a second credential;

a third data field that represents a chain of semantics inheritance between the first and second credential.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

44. In a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for a source computing system constructing an electronic message, the method comprising the following:

an act of encoding a credential that identifies the source computing device;

an act of including the credential in a header portion of an electronic message; and

an act of including, in the header portion, information indicative of a type of the credential.

45. A method in accordance with Claim 44, wherein the information indicative of a type of the credential comprises a human-readable expression of the type of the credential.

46. A method in accordance with Claim 44, wherein the information indicative of a type of the credential comprises information that is not a human-readable expression of the type of the credential, but nonetheless is information from which the type of credential may be derived.

47. A method in accordance with Claim 44, further comprising the following:

an act of including in the header portion, an identification of an encoding format of the credential.

48. A method in accordance with Claim 44, wherein an identification of an encoding format of the credential is not included in the header portion thereby indicating that a default encoding format has been applied.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

49. The method in accordance with Claim 44, further comprising the following:

an act of including an encryption manifest in the header portion to thereby designate portions of a body portion of the electronic message that are encrypted.

50. The method in accordance with Claim 44, wherein the credential includes biometric data.

51. The method in accordance with Claim 44, wherein the electronic message is a Simple Object Access Protocol (SOAP) envelope, and wherein the header portion is a header portion of the SOAP envelope.

52. The method in accordance with Claim 44, wherein the electronic message is a HyperText Transport Protocol (HTTP) message, and wherein the header portion is a header portion of the HTTP message.

53. A method in accordance with Claim 44, wherein the credential is a license.

54. A method in accordance with Claim 53, wherein the credential is in a binary format, wherein the act of including, in the header portion, an identification of a type of the credential comprises an act of including, in the header portion, an indication that the credential has the binary format.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

55. A method in accordance with Claim 44, wherein the credential is in a binary format, wherein the act of including, in the header portion, an identification of a type of the credential comprises an act of including, in the header portion, an indication that the credential has the binary format.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

56. A computer program product for use in a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, the computer program product for implementing a method for a source computing system constructing an electronic message, the computer program product comprising one or more computer-readable media having stored thereon the following:

a first software module that, when executed by one or more processors, is adapted to encode a credential that identifies the source computing device;

a second software module that, when executed by one of more processors, is adapted to include the credential in a header portion of the electronic message;

a third software module that, when executed by one of more processors, is adapted to include, in the header portion, an identification of an encoding format of the credential; and

a fourth software module that, when executed by one of more processors, is adapted to include, in the header portion, an identification of a type of the credential.

57. The computer program product of Claim 56, wherein the one or more computer-readable media are physical storage media.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

58. In a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for a source computing system constructing an electronic message, the method comprising the following:

an act of including an electronic signature in a header portion of an electronic message, the electronic signature generated by a user;

an act of generating a reference indicating where a credential associated with the electronic signature may be found;

an act of including the reference in the header portion of the electronic message.

59. The method in accordance with Claim 58, further comprising the following:

an act of including an encryption manifest in the header portion to thereby designate portions of a body portion of the electronic message that are encrypted.

60. A method in accordance with Claim 58, wherein the reference indicates that the associated credential may be found at a location that is internal to the electronic message.

61. A method in accordance with Claim 58, wherein the reference indicates that the associated credential may be found at a location that is external to the electronic message.

62. The method in accordance with Claim 58, wherein the credential includes biometric data.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

63. The method in accordance with Claim 58, wherein the electronic message is a Simple Object Access Protocol (SOAP) envelope, and wherein the header portion is a header portion of the SOAP envelope.

64. The method in accordance with Claim 58, wherein the electronic message is a HyperText Transport Protocol (HTTP) message, and wherein the header portion is a header portion of the HTTP message.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

65. In a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for a recipient computing system to verify the identity of a sender of an electronic message, the method comprising the following:

an act of receiving the electronic message;

an act of reading an electronic signature from a header portion of the electronic message, the electronic signature generated by a user;

an act of reading a reference from the header portion, the reference indicating where a credential associated with the user may be found;

an act of using the reference to find the credential; and

an act of determining if the credential corresponds with the electronic signature.

66. A method in accordance with Claim 65, wherein the reference indicates that the associated credential may be found at a location that is internal to the electronic message.

67. A method in accordance with Claim 65, wherein the reference indicates that the associated credential may be found at a location that is external to the electronic message.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

68. A computer program product for use in a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, the computer program product for implementing a method for a recipient computing system to verify the identity of a sender of an electronic message, the computer program product comprising one or more computer-readable media having thereon the following:

computer-executable instructions for detecting the receipt of the electronic message;

computer-executable instructions for reading an electronic signature from a header portion of the electronic message, the electronic signature generated by a user;

computer-executable instructions for reading a reference from the header portion, the reference indicating where a credential associated with the user may be found;

computer-executable instructions for using the reference to find the credential; and

computer-executable instructions for determining if the credential corresponds with the electronic signature.

69. The computer program product of Claim 68, wherein the one or more computer-readable media are physical storage media.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

70. In a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for a source computing system constructing a Simple Object Access Protocol envelope, the method comprising the following:

an act of designating at least one destination address in the SOAP envelope, the destination address corresponding to one or more recipient computing devices; and

an act of including a first security token in a header portion of the SOAP envelope, the first security token being at least derived from a first credential of a first credential type.

71. The method in accordance with Claim 70, further comprising the following:

an act of including a second security token in the header portion of the SOAP envelope, the second security token being at least derived from a second credential of a second credential type.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111